



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/838,123	04/20/2001	Noel D. Matchett	000505	8687

38834 7590 09/07/2005

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER

LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/838,123

Applicant(s)

MATCHETT ET AL

Examiner

Samson B. Lemma

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 June 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 13-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 13-31 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

10

Art Unit: 2132

DETAILED ACTION

1. This office action is in replay to an amendment filed on June 09, 2005.

In the previous preliminary amendment made by the applicant Claims 1-12 have been cancelled and new **claims 13-31** have been added by the applicant. Only the new **claims 13-31** are pending.

Response to Arguments

2. Applicant's arguments with respect to **claims 13-31** have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 13-31** are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas J. Roberts (hereinafter referred as **Roberts**) (U.S. Patent No 5,008,935) in view of the publication paper by **Michael Portz**, title "On the Use of Interconnection Network in Cryptography ".(hereinafter referred as **Portz**) (Publication **1991**) (reference U)

Art Unit: 2132

5. **As per claim 13,25-27 and 31 Roberts discloses in a device for performing the Data Encryption Standard (DES) on a block of data bits under control of a DES key, [Abstract] (the blocks are encrypted under the control of a first key using any block encryption method such as the Data Encryption Standard DES) the combination with a modified "P" permutation in the "f function.[Abstract] (individual bytes of the encrypted blocks of a buffer are then permuted under the control of a second key to form an encrypted buffer)**

Roberts does not expressly disclose

- The modified permutation "P is actually inside the "f function of the DES.

However, in the same field of endeavor, **Portz** discloses that interconnection networks gives the opportunity to access and perform permutations at the same time.[Page 301 or the 1st page, 1st paragraph, lines 3-5]. **Portz** further discloses that an interconnection network is build up from switching elements (called β -element). Whether the inputs should be exchanged in the specific switching element or not is determined by a control-setting function h.[Page 307, reference "2.1" "Control strategy", lines 1-5]. **Portz** further teaches choosing a specific control-setting function h, means choosing a specific permutation from the set.[Page 307, reference "2.2 Topology, lines 1-12]. Furthermore **Portz** teaches cryptosystems like DES usually describes sets of fixed permutations and a solution to this is dealing with the virtual interconnection network, which could be derived from the topology. [Page 308, reference 2.3,"Virtual Interconnection Networks", lines 5-6] (What is disclosed by Portz as indicated above, is similar to the core concept of the invention mentioned by the applicant as recited in the abstract.)

Art Unit: 2132

It would have been obvious to one having ordinary skill in the art at the time the invention was made to replace the fixed permutation of the conventional DES with the variable permutation of the interconnection network as per teachings of **Portz** and combine it into the method taught by **Roberts** in order to strengthen the security of Data encryption standard(DES).

6. **As per claims 14**, the combinations of **Roberts and Portz** discloses the improved device as applied to claim 13, above. Furthermore **Roberts** discloses the improved device includes a second cipher key to specify said modified "P" permutation. [Abstract] (individual bytes of the encrypted blocks of a buffer are then permuted under the control of a second key to form an encrypted buffer)

7. **As per claims 15**, the combinations of **Roberts and Portz** discloses the improved device as applied to claim 13, above. Furthermore **Portz** discloses the improved device includes a logic gates for implementing said modified "P" permutation.[Page 308, figure 5]

8. **As per claims 16-20 , 23 and 29**, the combinations of **Roberts and Portz** discloses the improved device as applied to claim 13 and 27, above. Furthermore **Portz** discloses the improved device wherein said modified "P" permutation is selected by a control signal.[Page 307, reference 2.1, Control Strategy and reference 2.2, Topology, lines 3-5](Choosing the control-setting function h means choosing a specific permutation from this set.)

9. **As per claims 21-22**, the combinations of **Roberts and Portz** discloses the improved device as applied to claim 15, above. Furthermore **Portz** discloses the improved device wherein said logic gates comprise a Benes-Waksman network.[figure 5]

Art Unit: 2132

10. **As per claims 24**, the combinations of **Roberts and Portz** discloses the improved device as applied to claim 13, above. Furthermore **Portz** discloses the improved device wherein including said DES key and a second cipher key.[column 1, lines 54-63]
11. **As per claims 28**, the combinations of **Roberts and Portz** discloses the improved device as applied to claim 27, above. Furthermore **Portz** discloses the improved device wherein the modified permutation is dependent upon a second cipher key. [column 1, lines 54-63; Abstract]
12. **As per claims 30**, the combinations of **Roberts and Portz** discloses the improved device as applied to claim 13, above. Furthermore **Portz** discloses the improved device wherein said modified permutation is a function of a subset of said DES key and a second cipher key. [column 1, lines 54-63; Abstract]

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

Art Unit: 2132

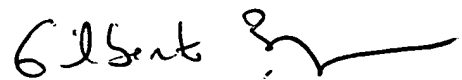
published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.

08/29/2005



GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100